(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 November 2003 (13.11.2003)

PCT

(10) International Publication Number
WO 03/093951 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US03/14204

(22) International Filing Date: 5 May 2003 (05.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/380,153 4 May 2002 (04.05.2002) US

(71) Applicant *(for all designated States except US)*: **INSTANT802 NETWORKS INC.** [US/US]; 1000 Marina Boulevard, Suite 400, Brisbane, CA 94005 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BARBER, Simon** [US/US]; 517 Mississippi Street, San Francisco, CA 94107 (US). **PETRUSCHKA, Roy** [US/US]; 185 Forest Avenue, Unit 4A, Palo Alto, CA 94301 (US). **DeCASTRO, Edward, Rodriguez** [US/US]; 2729 Lombard Street, #10, San Francisco, CA 94123 (US).

(74) Agents: **ALBERT, Philip, H.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

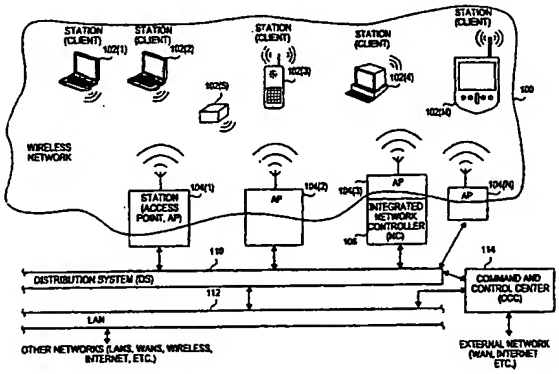
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** IMPROVED ACCESS POINT AND WIRELESS NETWORK CONTROLLER



(57) **Abstract:** In a wireless network, access points are used for monitoring radio spectrum traffic and interference thereof in a wireless network, managing control functions (access control, user management, radio management, tunnelling, etc.) A command and control center (CCC) is generally associated with the wireless network, wherein the CCC manages and controls the access points associated with the wireless network. Control frames (MMPDUs, in the case of 802.11 networks) received by the access point can be automatically transferred to the CCC, which thereafter transfers a response back to the access point, thereby granting or denying access to the wireless network to users thereof based on the response transferred from the CCC. The CCC manages radio monitoring to generate a radio mapping of the wireless network and the radio environment thereof based on data received from the access points. A firewall is generally located between the CCC and a visitor gateway. The visitor gateway can communicate with the Internet and restrict access to the wireless network by a visiting user through or from the remote computer network. A plurality of clients can be separated into one or more client groups, with each client group possessing a shared key for accessing networks partitioned from the access point using broadcast frames and encryption. The CCC can arrange the network such that clients ignore broadcast packets for other than its subnetwork.

WO 03/093951 A2

[0006] Networks, protocols and standards are typically designed and specified according to a now standard seven-layer ISO/OSI network model. Within that model, the 802.11 standard generally focuses on the MAC (medium access control) layer and the PHY (physical) layer.

[0007] 802.11-compliant communication occurs between stations. Some stations serve as access points between a wireless medium and a distribution system other than the wireless medium, while other stations only use the wireless medium to communicate 802.11 data. An example of a distribution system is a wired local area network (LAN), such as an Ethernet-protocol LAN, the Internet, or other network. The distribution system might even be another wireless system (which might be useful to support a number of nodes that can access the access point wirelessly, but not the wireless medium that is used as that access point's distribution system). The same wireless network might also serve as the distribution system (DS) using "wireless DS" transport.

[0008] While an access point is a station according to the 802.11 standard if it interacts with the wireless medium, the term "station" is often informally used to refer to a network node that is not connected to a distribution system and the term "access point" is used to refer to a station/node that is connected to a distribution system, thus allowing a distinction between nodes that can access a distribution system outside the wireless medium and those that cannot. That convention is used hereinafter, unless otherwise indicated.

[0009] Wireless networks with multiple stations but no access points are referred to as "ad-hoc" networks. Without more, an ad-hoc network allows for communication among stations accessible via a wireless medium, but not for communications beyond that ad-hoc network.

[0010] In an 802.11 wireless network with at least one access point, a station located within a group or cell sends packets of data to the access point, which in turn forwards messages/packets/data to a destination such as a station within the same cell or, via the access point's distribution system, to a destination outside the wireless medium.

[0011] The 802.11 standard generally supports several data signalling schemes: DSSS (direct sequence spread spectrum) with differential encoded BPSK and QPSK; FHSS (frequency hopping spread spectrum) with GFSK (Gaussian FSK); OFDM (orthogonal frequency division multiplexing, infrared with PPM (pulse position modulation) are several examples. DSSS, FHSS and infrared all provide bit rates of 1 Mbs (megabits per second) and 2 Mbs. The 802.11b extension provides for a high rate CCK (Complementary Code Keying) physical layer protocol, providing bit rates of 5.5 and 11 Mbs as well as the basic DSSS bit rates of 1 and 2 Mbs within the 2.4-2.5 GHz ISM band. The 802.11a extension provides for a high bit rate OFDM (Orthogonal Frequency Division Multiplexing) physical layer protocol

[0015] When a wireless LAN station is powered on, it first looks for an access point. After it finds an access point, the wireless LAN station registers itself with the access point (authentication, association). The station can then synchronize with the access point and, thereafter, transmit and receive data frames to and from the access point. In a common example, the client station is a portable or mobile computer with a wireless networking card installed therein. 802.11 management frames are used to set up these connections.

[0016] Unlike wired networks, where a network is secured at boundaries by which wires connect to the network, wireless networks do not have well-defined boundaries. A company on one floor of a building might have a wireless network that can be reached by a computer on a different floor using a computer unrelated to the company that set up the wireless network. Consequently, it is easier to join into a wireless network, for authorized users as well as unauthorized users.

[0017] In some cases, a wireless network could be coupled to a wired network without oversight by the operators of the wired network. For example, many access points have a standard interface and can be easily plugged into a standard wired network connector, thus opening up a previously secured wired network to wireless traffic. Where an uninformed end-user replaces a wired network connection with an access point and does not secure the access point, the wired network would then be open to users within radio range of the access point, even if they were not within the physical space controlled by the organization for which the wired network is being maintained.

[0018] Some network operators have attempted to address unexpected access points by physically surveying their network. In one approach, a network administrator would walk with a network sniffer through all of the space controlled by the organization, but for large spaces, this is often impractical.

[0019] In large wireless networks, considerable effort is needed to maintain numerous access points and when a large number of access points are needed, for bandwidth reasons, coverage reasons, etc., the cost can be considerable as the full functionality of an access point needs to be repeated in the space where the network is set up.

[0020] Another difficulty of wireless networks is that of not necessarily authorized users in the authorized space. For example, if a visitor with a wireless computer or wireless device is in a company building that is covered by the company's wireless network, that visitor might connect to the company network and have access equivalent to that of an employee, and that is generally undesirable.

[0026] A further understanding of the nature and the advantages of the inventions disclosed herein may be realized by reference to the remaining portions of the specification and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] The accompanying figures, in which like reference numerals refer to identical or functionally-similar elements throughout the separate views and which are incorporated in and form part of the specification, further illustrate the present invention and, together with the detailed description of the invention, serve to explain the principles of the present invention.

[0028] FIG. 1 is a block diagram of a wireless network and components to support the network according to the present invention.

[0029] FIG. 2 is a block diagram showing elements of Fig. 1 in greater detail.

[0030] FIG. 3 illustrates several variations of communication paths between an access point and a command and control center (CCC).

[0031] FIG. 4 illustrates several data tables maintained by an access point according to aspects of the present invention.

[0032] FIG. 5 illustrates an access point monitoring radio traffic under control of the CCC.

[0033] FIG. 6 is a swim diagram illustrating interactions between two access points and the CCC for radio monitoring and mapping.

[0034] FIG. 7 is a graphical representation of the results of a radio map, wherein several access points determine statistics of signals from objects in the wireless network space.

[0035] FIG. 8 illustrates how radio map statistics could be used to at least approximately locate an access point at a physical location.

[0036] FIG. 9 illustrates several data tables that might be maintained by a CCC to improve network connections and user experiences.

[0037] FIG. 10 is a flowchart of a process for diagnosing user problems based on network history.

[0038] FIG. 11 is a swim diagram illustrating interactions between a client, an access point and a CCC, where access is controlled centrally by the CCC.

[0039] Fig. 12 illustrates tunnelling used in a wireless network.

[0040] Fig. 13 illustrates broadcasting to subnetworks of a wireless network using encryption.

addresses to create and update routing tables and network data structures and to determine whether a particular frame is directed at that device or where to direct a particular frame. The term "MAC address" can be utilized interchangeably with the term "link layer address".

[0046] While it might be common to the point of being a convention that addresses on a wireless network and communication systems outside of the wireless network that are connected to the wireless network are addresses that are compatible and unique across the entire system, the present invention is not necessarily limited to such addressing schemes although many of the examples herein assume a unified, coordinated address space. Such unification has its advantages, allowing for simple bridging from wireless to IEEE 802 wired networks.

[0047] Generally, data being communicated herein is assumed to be in the form of digital transmissions. However, it should be understood that such data can take a number of forms, such as bits, values, elements, symbols, characters, terms, numbers or the like, and can be represented as electrical or magnetic signals, states of storage elements, or the like. It is also assumed that physical signals can either be represented as analog electrical or magnetic signals, stored state, digital samples represented by numbers of predefined precision, a time sequence of such digital samples, or the like.

[0048] The present invention should not be construed as being limited to any particular data form or representation, although it is generally understood that the data physically exists and is capable of being stored, transferred, combined, compared, and otherwise manipulated by physical processes. Further, manipulations performed are often referred to in terms that are commonly associated with mental operations performed by a human operator, even though the manipulations can only be practically performed as machine operations. Useful machines for performing operations of the present invention include data-processing systems, such as general-purpose digital computers, server-based devices, handheld devices, embedded devices, wireless and/or wireline networks, or other similar devices and systems thereof. In all cases, the distinction between the method of operations in operating a computer and the method of computation itself should be borne in mind.

[0049] Throughout this specification, aspects of the disclosure are described by block diagrams, swim diagrams and flowcharts. Where an element is shown in a block diagram by a simple box, it should be understood that the element could be made and used with the reference to the entire specification and knowledge available to one of ordinary skill in the art. The swim diagrams illustrate interactions between two or more elements in a particular time order. Unless otherwise indicated, it should be understood that some of the interactions

[0053] It can be additionally appreciated by those skilled in the art the system and/or method described herein can be implemented as a single module or a series of modules. Such modules can be utilized separately or together to form a program product that can be implemented through signal-bearing media, including transmission media and recordable media. A module can be stored, for example, within a memory location of a server and processed via associated processors or microprocessors thereof. Such modules may also control and command functions associated with such a server or devices in communication with the server.

[0054] The term "user management" generally refers to activities that involve the identification of a network user, the type of network privileges associated with that network user, and the level of service that the user should be receiving. The term "radio management" generally refers to telecommunications activities taking place within a wireless network. For example, radio management can include a determination of the access point (AP) communicating with a device having a particular MAC address, along with the type and location of the service being provided.

[0055] In the examples described herein, the wireless network is an IEEE 802.11 network, but it should be clear that other networks and variations of IEEE 802.11 networks could be used instead. Each network device is referred as to a "station". Stations that derive their connectivity solely through the wireless network are referred to herein as "clients" and stations that connect to networks outside of the wireless network and are usable to carry traffic from clients to such networks are referred to herein as "access points". Of course, a client might have other techniques for communication outside the wireless network, but it is assumed that the client does not carry data for other device is in the wireless network. For example, a cellular telephone that is enabled for communication over a wireless network might be described as a client even the now the cellular telephone is able to communicate through a telephone network independent of the wireless network. The term "outside network" is used herein to refer to communications channels other than the wireless network being described where the outside network might be the destination of some of the traffic of the wireless network. Thus, clients that communicate over a wireless network will communicate to an access point that carries the communication over the outside network. The outside network could itself be a wireless network.

[0056] The above concepts should be kept in mind in understanding the figures and their description below.

client. For an access point to allow an association, the client needs to authenticate itself to the access point (in some networks, anyone can connect).

[0063] Fig. 2 illustrates one client 102, one access point (AP) 104, and one CCC 114 in greater detail. It should be understood that a typical wireless network would include a plurality of clients and a plurality of access points, and possibly also a plurality of CCCs.

[0064] As shown in the figure, AP 104 comprises a processor 202, program code 204, data store 206, a network interface to receive data from and said data to other network devices such as client 102, an interface to communicate with CCC 114, any interfaces as needed for other communications, such as communications with a distribution system (DS) and a local area network (LAN). Other elements, components and modules might be present in AP 104, but are not shown.

[0065] Program code 204 is shown including a network state module 210, a radio monitoring/mapping module 212 and a standard service set module 214. Standard service set module 214 can perform the functions typically found in conventional access points, and as such, need not be described in detail here. Other modules might be present, but are not shown. Data store 206 is shown comprising several data objects, such as a clients table 220, a radio stats table 222, a broadcast keys table 224, and other data objects not shown.

[0066] CCC 114 is shown in comprising a control module 240, a radio monitor/mapper module 242, a diagnostic subsystem 244, a link layer authenticator 246, a network management module 248, and a list of active/supported clients 250. Other modules and data structures are present in CCC 114 but are not shown. As indicated, CCC 114 can communicate with a distribution system, a LAN (such as a corporate network), a WAN, the Internet, or the like.

[0067] CCC 114 can perform a number of functions, such as controlling access to the wireless network, managing radio mapping and otherwise monitoring, controlling, evaluating, reconfiguring, etc. the wireless network for optimal performance, security and user satisfaction. As illustrated in Figs. 1-2, clients interact with access points and access points interact with the CCC. Access points generally function as the points on the edge of wireless network 100 and CCC controls those access points. In a typical wireless network, there will be more access points than CCCs, so centralizing some functions traditionally performed by access points into the CCC allows for less expensive access points, simpler maintenance and oversight of the network, and a number of other benefits.

[0068] Fig. 3 illustrates a number of variations for communication between an access point and a CCC. Fig. 3(A) shows communication via a distribution system (DS). The medium to

areas, etc. Physical monitoring, such as by a technician moving through the wireless network space, is time-consuming and might interfere with normal operation of the network.

[0074] Fig. 6 illustrates one possible sequence for mapping a wireless network. In a sequence, the CCC performs a passive listening process, then an active mapping process, and then a scan process. These processes can be done in that different orders or be done separately. As illustrated, in step S1, the CCC directs the access point to begin the passive listening process. The access point begins the process (S2) listening for frame traffic and non-frame traffic and populates its radio stats table (see Fig. 4(B)) accordingly. For each is source of radio signal, the access point might be able to identify it as a station or as a non-station source of interference. For stations, the access point should be able to identify an SSID for the radio, whether it is an access point, if it is a client, whether it is associated with the access point, and various other measurement parameters. These radio stats are gathered and reported back to the CCC (S3), which then can analyze them (S4) to determine the nature of a radio sources in the wireless network.

[0075] When requesting active mapping (S5), the CCC would issue a particular mapping command or set of mapping commands to the access point, which would then receive the command or commands (S6) and form suitable mapping frames to be transmitted (S7) over the wireless network in support of those commands. Some of the mapping frames can be expected to be received by other access points. Those other access points, specifically the radio modules of those access points, would then receive the mapping frames (S8), gather radio and MAC stats for those frames (S9), and report the results back to the CCC (S10). The CCC could then analyze the radio and MAC stats (S11).

[0076] For a scan process, the CCC sends a request for a scan over multiple channels, multiple frequency bands, or combination thereof, to the access point (S12). The access point then receives a request (S13) and sequences through the channels and/or frequencies and listens for traffic and/or sends out mapping frames, gather radio stats to be reported back to the CCC (S14), which then can analyze the stats (S15) and perform other tasks (S16).

[0077] In this manner, a survey can be done of the wireless network. One interesting result of a survey is that the CCC can detect "rogue" access points that are using the wireless network but are unknown to the CCC. Rogue access points can be the result of an unauthorized user adding the access point to a network, interference from neighboring wireless networks, or authorized access points not yet configured or registered.

[0078] Preferably, radio monitoring does not interfere with normal network operations. For example, it would be unwise for an access point that is serving four or five active users to

[0083] Fig. 7 is a logical representation of such a radio map. As shown there, the wireless space includes two access points, AP1 and AP2, that are known to be connected to a LAN 704, two clients (A, B), two access points, APx and APy, known to be connected to an unrelated neighboring network 706 and an access point, AP?, of unknown origin. In one representation, the radio map has links 700 and stats 702 for each link, where a link represents traffic from one source to one monitoring access point. Note that some of the sources might be other than network devices. Examples of stats for a link might be as shown in Fig. 4(B). As illustrated, AP1 has detected the presence of client A, client B, access point AP2, access point AP?, and access points APx and APy, while AP2 has detected the presence of client A, client B, access point AP1, access point AP?, access point APy, and non-network interference sources. For each of these presences, the respective access point can record statistics and forward them to the CCC.

[0084] With a collection of data for radio sources, the CCC might be able to determine an approximate mapping. For example, consider Fig. 8. Assume that distance between two radio sources is determinable from signal strength. That is often not the case for wireless networks, with differing transmit powers, multipath interference, signal delays, and the like, but it is illustrative nonetheless. With information from AP1, the CCC can determine the distance from AP1 to AP3 and the distance from AP1 to AP2, and can do likewise for the other two access points. From those distances (and the absolute location of at least one source in the wireless network), the CCC might be able to determine the location of each of the other access points. Of course, given the typical environment expected of a wireless network, the signals will not be perfect, but with many access points providing additional data points, the location of each access point could be determined at least approximately enough to allow a technician to quickly locate and/or isolate any given radio. With such information, for example, a network administrator can quickly zero in on a rogue access point.

[0085] Other conclusions can be derived from the radio map. For example, areas of poor coverage may be detected, which in turn permits the CCC to recommend the placement of additional access points based on data compiled the real-time map. Such a map also permits the detection (i.e., area/time/date/frequency channels) of known radio sources of radio disturbances (e.g., 12:00, weekdays, all channels, around the second floor, cafeteria, etc.) and the generation of corresponding alerts. Any neighboring networks can also be detected based on data contained with the generated real-time map. In addition, the transmission channels,

point might be dedicated to the radio stats collection process such that it does not carry client traffic, just monitors radio traffic and/or actively probes the wireless network. In some cases, an access point will monitor just frames addressed to that access point, while in others the access point just or also monitors frames that are addressed to other network devices. In some cases, the access point just records information that a conventional access point would record, but in other cases, the access point records more data than is normally needed to act as an access point or saves data that is developed in the PHY or MAC layer but is discarded in normal course of supporting conventional 802.11 traffic. For example, radio signal strength might be data used in the PHY layer and discarded once valid frames are received, but that data can be saved and passed on to the CCC for analysis of the wireless network. An access point might include other functions involving sniffing the wireless network to which it has access.

[0091] Radio stats can be combined with SNMP an authentication data to get a fuller network state. This data can be used to deal with rogue access points or to adjust the network in other ways. For example, if the CCC finds that an unauthorized access point is operating in its wireless space, the CCC can alert an operator and narrow down a physical search for the unauthorized access point. The CCC might also do the same for unauthorized clients, gateways, etc. The CCC might also act directly to disable the rogue access point if it is on a wired network or distribution system controlled by the CCC.

[0092] In addition to dealing with rogue network devices, the CCC might also handle network reconfigurations. For example, based on radio stats, the CCC might determine that an access point is overloaded and make selective requests to that overloaded access point to deassociate one or more network devices. Preferably, the network devices that are to be disassociated are within range of other access points, a condition that the CCC can determine from the collection of radio stats from other access points. The CCC might be used to monitor other, more complex statistics, such as a comparison of airtime usage versus throughput.

[0093] Fig. 9 illustrates several tables that might be used by the CCC to support a user radio and a link management process. Fig. 9(A) is a table of active clients indicating, for each active client, the user MAC address, actual physical location (as that might be estimated during a radio survey), expected physical location (as might be determined during a physical installation process), a list of active services for that client, and other parameters about the client. Fig. 9(B) is a table of historical network activity usable for diagnostics and support.

the network using differing devices). Additionally, such services can permit the use of such information to ensure (rather than simply monitor) the quality experienced by person a particular network user, regardless of the device/MAC address they are using. In addition, such services can include the ability to track down multiple failed connection attempts by a certain MAC address and deduce the user who is failing to connect (e.g., the user may have lost a password) based on historical connection data and proactively call/email the user(s) with support. Finally, such services may include a tying of association of specific user trouble-tickets with specific events at the network level, such as for example, transmission types and rates, association/disassociation events and so forth.

[0099] Fig. 11 is a swim diagram illustrating another use of the CCC, to provide centralized access control. The process begins with a client sending a MAC management frame (S110) to an access point. Previous access points might have processed the request locally, which in turn is sent out across an associated wired network to an authentication authority (e.g., a domain server or a directory) and base its decision on data returned by the authentication authority. With the present approach, the access point transfers of the decision-making process to the CCC forwarding the control frame (S111) to the CCC. The CCC receives a control frame (S112) and determines if the clients is to be given access (S113). If the client is not to be given access, the CCC responds (S114) to the access point to deny the client (S115) and the client receives a denial (S116). In some instances, clients are not informed of the denial and only hear from the access point when access is granted.

[0100] Where the CCC decides to grant access, it indicates to the access point that access is granted and provides indication of the permissions granted to the client (S117). The access point then initializes is a local tables for granting permissions as indicated by the CCC (S118) and sends an authentication response to the client (S119). Once the client receives the authentication response (S120) and continues with association and second authentication and other processes (S121).

[0101] As described above, the access points pass key management and control functions of 802.1x access points to a central controller (the CCC). This allows other functionality, such as the routing of visiting users away from private networks and tunneling between the client and the CCC through the access point. Communications between the CCC and the access point can be carried out through a secured tunnel (s-tunnel) connection. It can be appreciated that the access points can carry out a "firewall" function by passing any control frames (for 802.11, MMPDUs are examples of control frames) received from clients back to a dominating CCC that can control the access points in detail and assume the role of an

networks according to the present invention, multiple independent networks are supported through a set of access points use the existing 802.11 encryption protocols. 802.11 devices can send frames indicated as unicast frames, multicast frames, or broadcast frames. Unicast frames are characterized as having a single network device as its destination. Broadcast frames are characterized as being directed to all network devices that are capable of receiving the frames. Multicast frames are in between unicast frames and broadcast frames in that that multicast frames are characterized as having a destination that is a group with which network devices can be associated. Multicasting requires more infrastructure then the unicasting or broadcasting, as group associations need to be maintained.

[0107] Where multiple independent overlapping wireless networks exist, it is preferable to have technique for broadcasting just among one of the overlapping networks and to do so with the minimum amount of set up. Using a wireless network configured according to aspects of the present invention, this is done using the encryption behaviors of the typical wireless network. In a typical wireless network, network device receives frames and determines whether the frames are encrypted. If the frames are encrypted, the network device attempts to decrypt the frames using the encryption keys available to the network device. If the network device it cannot decrypt and encrypted frame, the network device drops the frame. In a typical instance, the network device will silently drop the frame (i.e., not request retransmission or otherwise indicate failure of receipt).

[0108] For unicast traffic, the access point could maintain a MAC address of each client in a table indicating which MAC addresses go with which distribution systems (Doss). However, for broadcast traffic, is more difficult for one access point to manage multiple sets of traffic among the stations associated with the access point. When an access point transmits a broadcast frame, all associated clients will receive and process that broadcast frame, which is undesirable when attempting to a broadcast a frame to just a subset of clients associated with less than all of the distribution systems served by the access point. The access point typically transmits broadcast frames and a unicast frames using a BSSID (typically, the MAC address of the access point's radio) that the client understands is the BSSID for the access point with which the client is associated.

[0109] To solve this problem, the network is configured to use 802.1x encryption processes to in effect "separate out" broadcast traffic for multiple networks. Thus, the clients that are part of a first network will have a first encryption key used for broadcast frames (and possibly some unicast frames) and clients that are part of a second network will have a second encryption key used for broadcast frames and other frames. When a particular client receives

send a broadcast message to all clients in the network 4, it would use the broadcast keys for network 4 and that message would be dropped by all clients except those in the network 4.

[0114] While the above example is explained with an illustration of multiple distribution systems (DS's), there might be some configurations where the traffic is carried on a single distribution system.

[0115] Stations that expect to receive encrypted traffic are generally set to reject unencrypted traffic, so it is thus possible to partition the access point into two independent networks. For example, a network device on a first independent network might be configured to ignore unencrypted traffic and receive broadcast messages encrypted with broadcast keys for the first independent network, while a network device on a second independent network might be configured without any broadcast keys and thus would only except the unencrypted traffic and discard the encrypted broadcast frames.

[0116] Novel access points, wireless network controllers, enhanced methods of wireless network control and the like have now been described. Some implementations might be in the form of novel access points, while others are in the form of additional functionality added to existing access points. For example, an access point that is implemented as a chipset and/or programmable devices might simply include added software to handle one or more of the novel functions described herein. Modifications might be made to clients, but the present invention can operate with conventional clients as well.

[0117] The embodiments and examples set forth herein are presented to best explain the present invention and its practical application and to thereby enable those skilled in the art to make and use the invention. Those skilled in the art, however, will recognize that the foregoing description and examples have been presented for the purpose of illustration and example only. Other variations and modifications of the present invention will be apparent to those of skill in the art, and it is the intent of the appended claims that such variations and modifications be covered. The description as set forth is not intended to be exhaustive or to limit the scope of the invention. Many modifications and variations are possible in light of the above teaching without departing from the spirit and scope of the following claims. It is contemplated that the use of the present invention can involve components having different characteristics. Many variations of the invention will become apparent to those of skill in the art upon review of this disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the appended claims along with their full scope of equivalents.

9. The system of claim 1, wherein the control module transfers the response back to the at least one access point thereby denying access to the wireless network to the user thereof based on the response transferred from the control module to the at least one access point.

10. A system for managing control functions associated with access points of a wireless network, the system comprising:

at least one access point associated with the wireless network, wherein the wireless network comprises an 802.11 wireless network;

a Control and Command Center (CCC) for managing and controlling the at least one access point associated with a wireless network, wherein at least one control frame received by the at least one access point is automatically transferred to the Control and Command Center (CCC), which thereafter transfers a response to the at least one access point thereby permitting access to the wireless network to a user thereof based on the response transferred from the Control and Command Center (CCC); and

a secure connection for securing communications between the Control and Command Center (CCC) and the at least one access point associated with the wireless network.

11. A method for managing control functions associated with access points of a wireless network, the method comprising the steps of:

associating at least one access point with the wireless network; and

establishing a control module for managing and controlling the at least one access point associated with a wireless network, wherein the control module communicates with the at least one access point associated with the wireless network;

automatically transferring at least one control frame received by the at least one access point to the control model; and

thereafter transferring a response to the at least one access point from the at least one control frame, in response to receiving the at least one control frame from the at least one access point, thereby permitting access to the wireless network to a user thereof based on the response transferred from the control module.

12. The method of claim 11, further comprising the step of:

configuring the control module to comprise a Command and Control Center (CCC) associated with the wireless network.

automatically transferring at least one control frame received by the at least one access point to the Control and Command Center (CCC);

thereafter transferring a response to the at least one access point to the Control and Command Center (CCC) based on the at least one control frame transferred from the at least one access point, thereby permitting access to the wireless network to a user thereof based on the response transferred from the Control and Command Center (CCC); and

establishing a secure connection for securing communications between the Control and Command Center (CCC) and the at least one access point associated with the wireless network.

21. In a wireless network wherein network devices communicate over a wireless medium and include access point devices that couple the wireless medium to a distribution system, an improved access point device comprising:

logic to listen to frames transmitted over the wireless medium;

logic to record statistics about receipt of the frames; and

logic to report the statistics to a controller for further analysis.

22. The apparatus of claim 21, wherein the logic to listen to frames transmitted over the wireless medium includes logic to listen to frames that are addressed to the improved access point device.

23. The apparatus of claim 21, wherein the logic to listen to frames transmitted over the wireless medium includes logic to listen to frames other than frames addressed to the improved access point device.

24. The apparatus of claim 21, wherein the logic to listen to frames transmitted over the wireless medium includes logic to listen to frames that are addressed to the improved access point device and to other network devices.

25. The apparatus of claim 21, wherein the logic to listen to frames transmitted over the wireless medium includes logic to listen to all frames that are correctly received by the access point.

26. The apparatus of claim 21, wherein the statistics include radio signal strength, radio signal quality, network device address, and interference type.

a network management module integrated with the link layer authentication module, such that the network management module and the link layer authentication module together form an integrated user and radio management module which provides wireless network services for the wireless network.

38. The system of claim 37, wherein the integrated user and radio management module permits a determination of a plurality of failed wireless network connection attempts based on a user address to thereby deduce a user associated with the user address.

39. A system for restricting access to a wireless network, comprising:

at least one access point associated with the wireless network;

a visitor gateway for automatically restricting entry of a visiting user to the wireless network; and

a command and control center associated with the wireless network, wherein the command and control center communicates with the at least one access point and the visitor gateway and controls data transfer and routing thereof.

40. A system for restricting access to an IEEE 802.11 wireless network, comprising:

at least one access point associated with the IEEE 802.11 wireless network;

a visitor gateway for automatically restricting entry of a visiting user to the IEEE 802.11 wireless network, wherein the visitor gateway communicates with a remote computer network and restricts access to the wireless network by a visiting user through the remote computer network; and

a command and control center associated with the IEEE 802.11 wireless network, wherein the command and control center communicates with the at least one access point and at visitor gateway and controls data transfer and routing thereof and wherein the command and control center automatically routes the visiting user to the visitor gateway when the visiting user attempts to access the at least one access point associated with the IEEE 802.11 wireless network;

a firewall located between the command and control center and the visitor gateway;

a protected zone in which access to and from the IEEE 802.11 wireless network is limited, wherein the visitor gateway is located within the protected zone of the IEEE 802.11 wireless network; and

the at least one wireless station to be partitioned into the at least one first wireless station and the at least one second wireless station.

47. The system of claim 43, further comprising:

at least one group of encrypted users who can access the wireless network through the at least one access point.

48. The system of claim 41, wherein the wireless network comprises an IEEE 802.11 wireless network.

49. The system of claim 41, wherein the at least one access point comprises at least one MAC address in association with at least one interface partitioned from the at least one access point.

50. A method of operating a plurality of independent networks using a set of one or more shared access points, the method comprising:

grouping network devices that are to use a wireless medium into the plurality of independent networks;

for each network device in one of the independent networks, providing a set of one or more keys usable to decode at least a portion of a received frame, wherein at least one network device is configured to drop broadcast packets that are not encrypted using one or more key from the set of one or more keys;

encrypting a frame using the one or more key for a current network, thereby forming an encrypted frame;

broadcasting the encrypted frame;

at a network device in the current network, receiving the encrypted frame and decrypting the received encrypted frame; and

at a network device not in the current network, receiving the encrypted frame and discarding the encrypted frame.

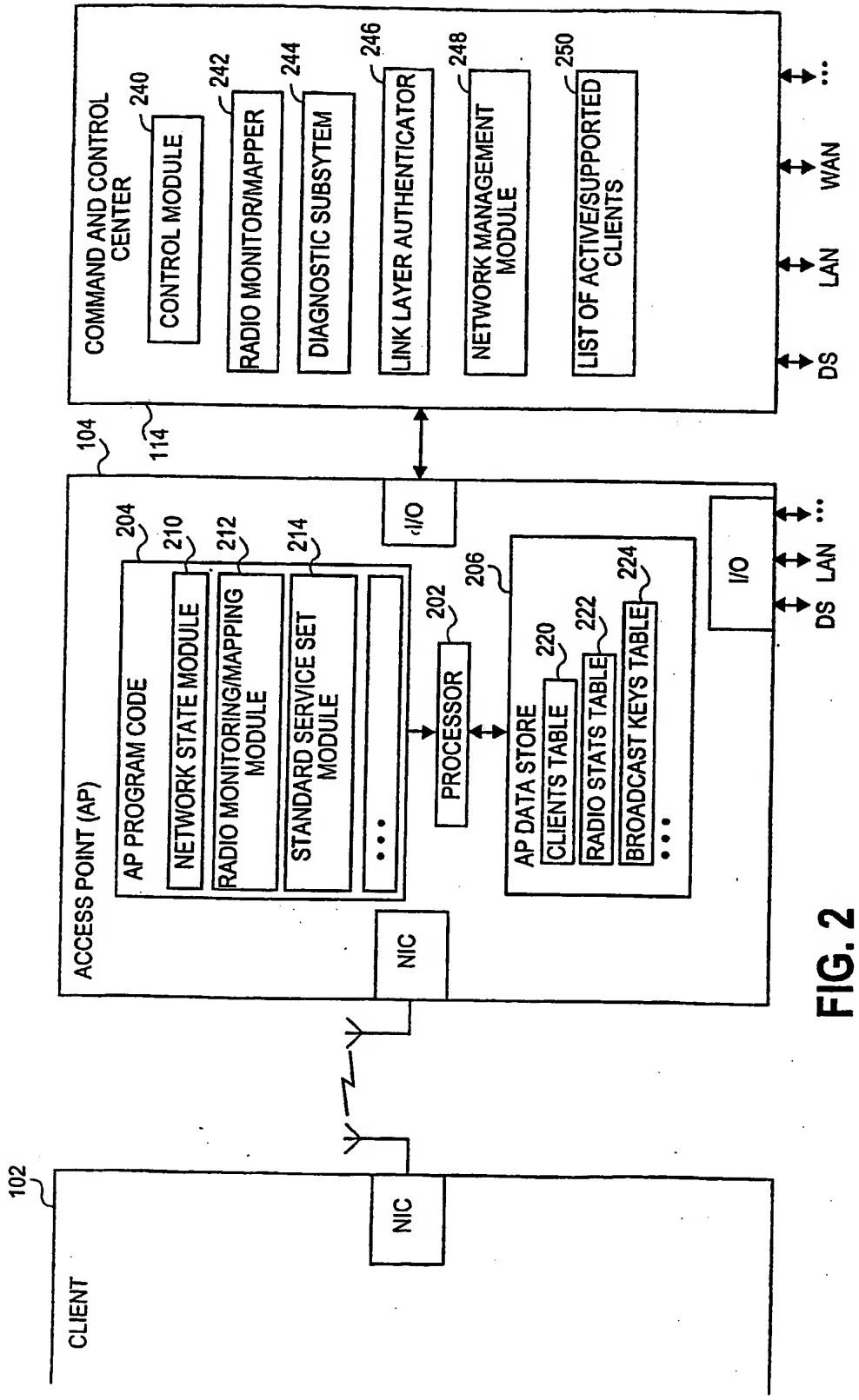


FIG. 2

ACTIVE CLIENTS TABLE 220

CLIENT SSID	NETWORK #	UNICAST KEY(S)	ROUTING INFO	• • •
		K1A, K1B, K1C, K1D		
• • •				

FIG. 4(A)

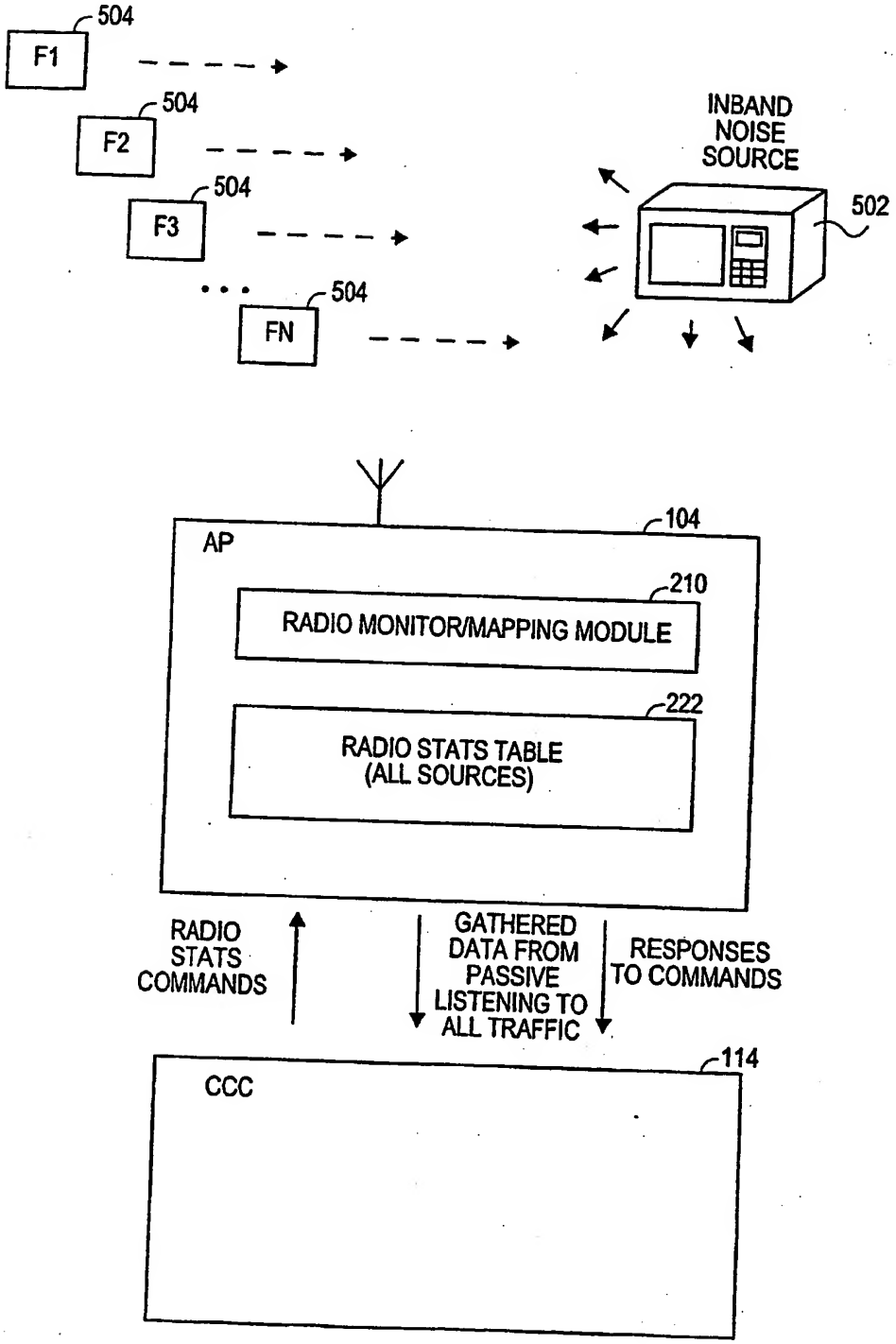


FIG. 5

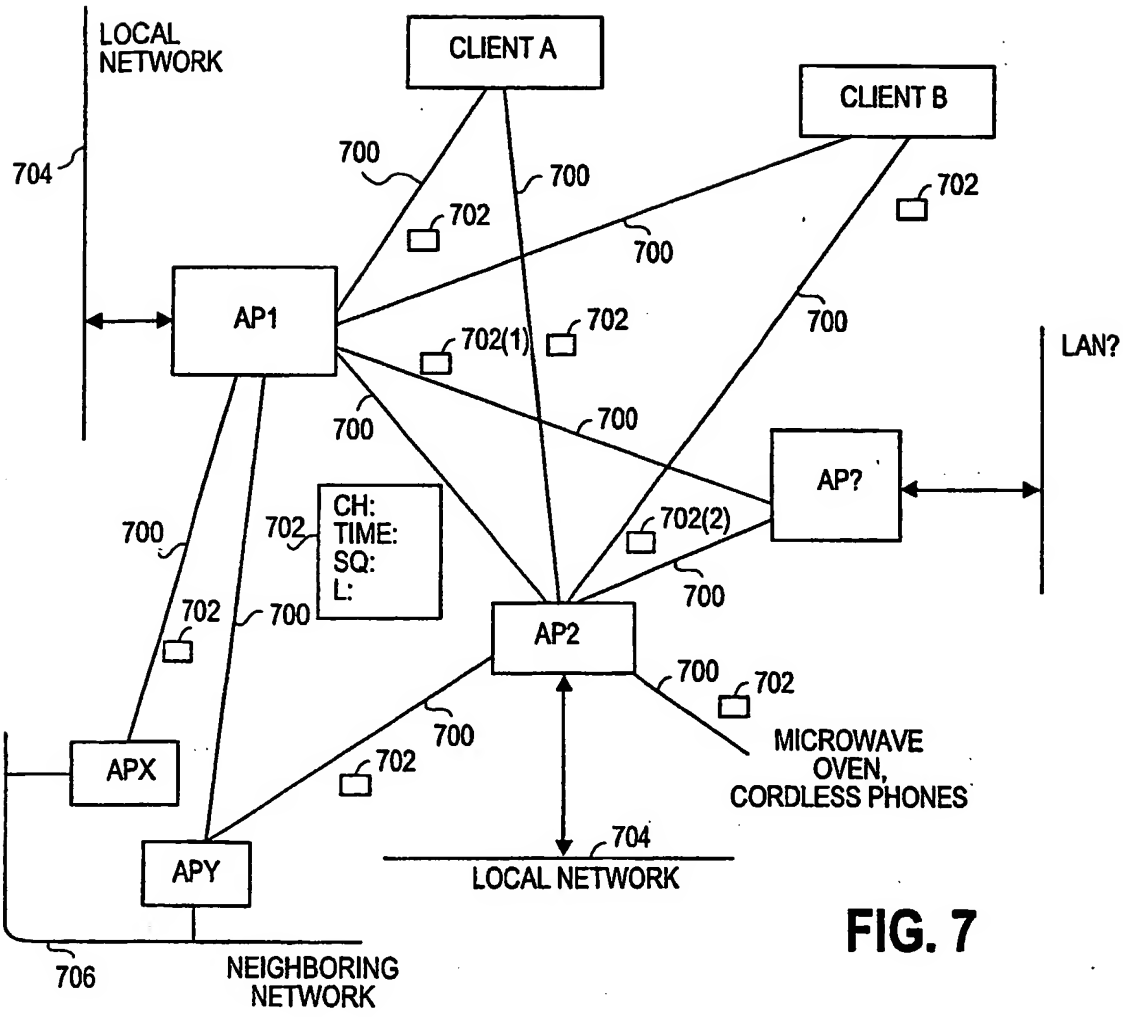


FIG. 7

USER MAC ADDRESS	ACTUAL PHYSICAL LOCATION	EXPECTED PHYSICAL LOCATION	ACTIVE SERVICE	...

FIG. 9(A)

USER MAC ADDRESS	HISTORICAL CONNECTION DATA	TROUBLE TICKETS		...

FIG. 9(B)

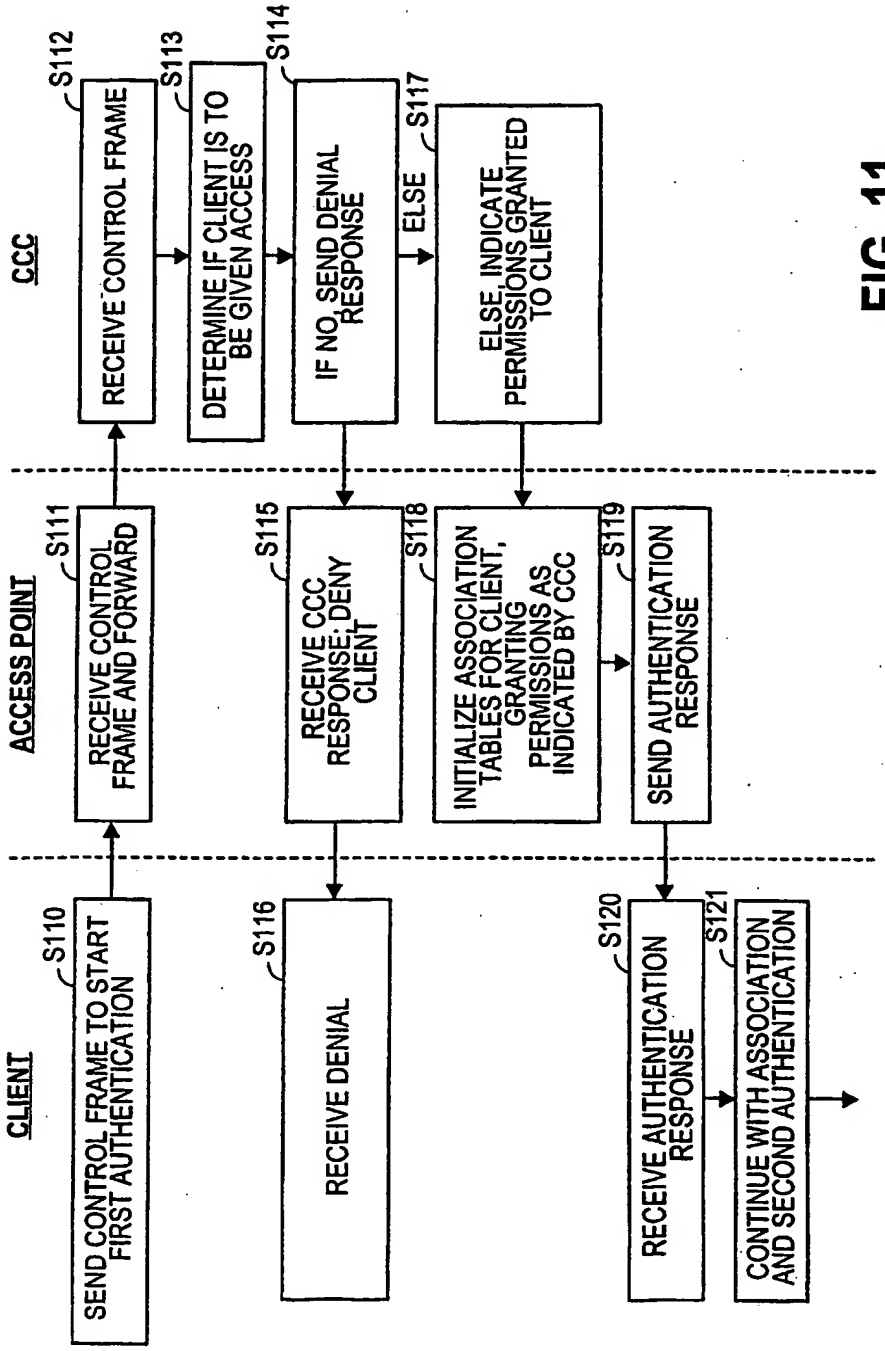


FIG. 11

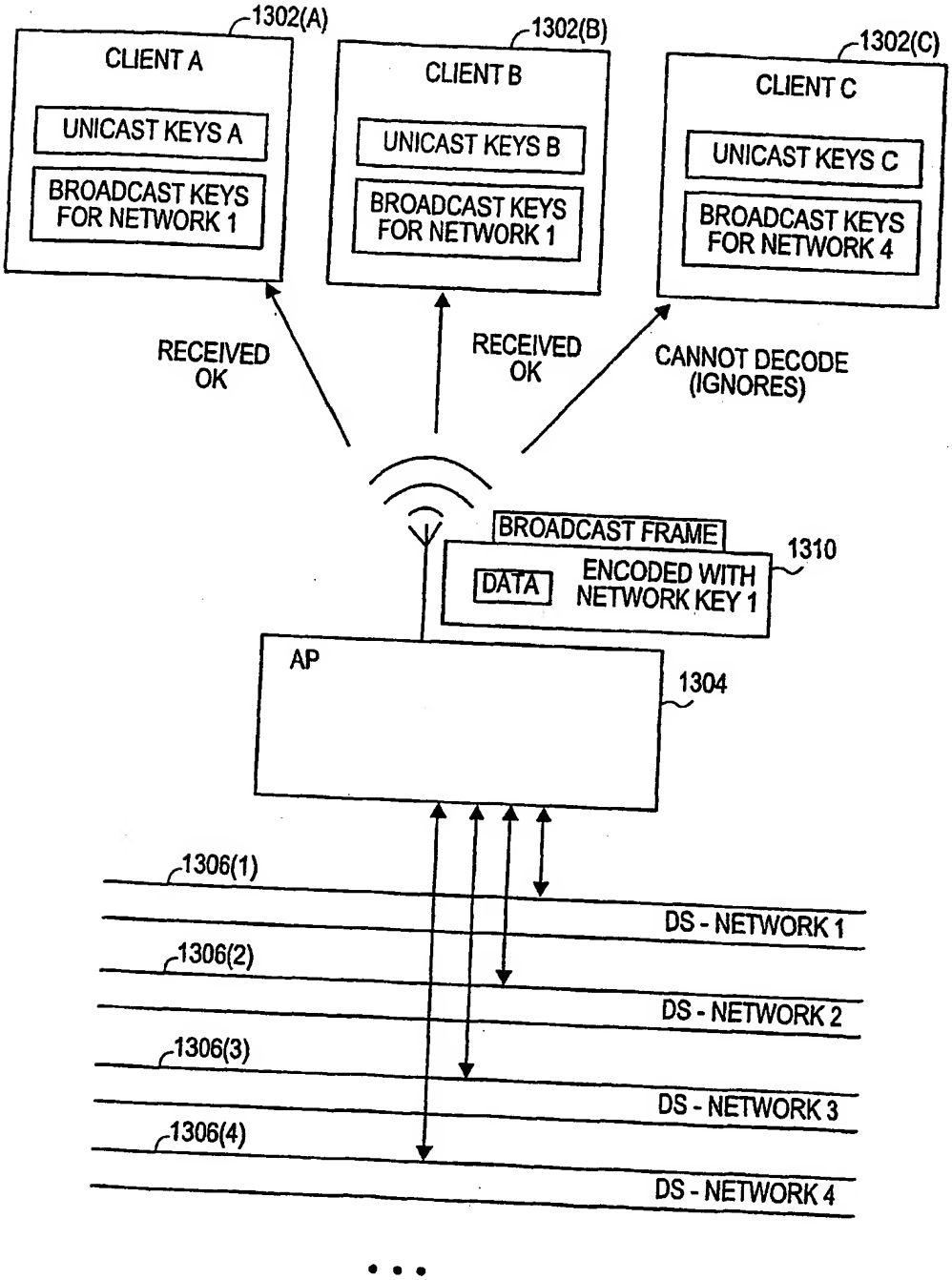


FIG. 13

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 November 2003 (13.11.2003)

PCT

(10) International Publication Number
WO 2003/093951 A3

(51) International Patent Classification[7]: H04L 12/56

(21) International Application Number:
PCT/US2003/014204

(22) International Filing Date: 5 May 2003 (05.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/380,153 4 May 2002 (04.05.2002) US

(71) Applicant *(for all designated States except US)*: **INSTANT802 NETWORKS INC.** [US/US]; 1000 Marina Boulevard, Suite 400, Brisbane, CA 94005 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BARBER, Simon** [US/US]; 517 Mississippi Street, San Francisco, CA 94107 (US). **PETRUSCHKA, Roy** [US/US]; 185 Forest Avenue, Unit 4A, Palo Alto, CA 94301 (US). **DeCASTRO, Edward, Rodriguez** [US/US]; 2729 Lombard Street, #10, San Francisco, CA 94123 (US).

(74) Agents: **ALBERT, Philip, H.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

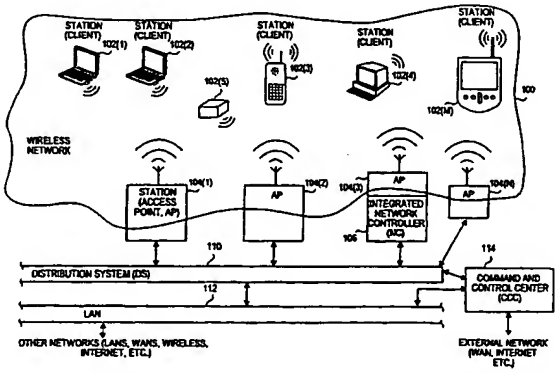
Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*

(88) Date of publication of the international search report:
8 April 2004

[Continued on next page]

(54) Title: IMPROVED ACCESS POINT AND WIRELESS NETWORK CONTROLLER



(57) Abstract: In a wireless network, access points are used for monitoring radio spectrum traffic and interference thereof in a wireless network, managing control functions (access control, user management, radio management, tunnelling, etc.) A command and control center (CCC) is generally associated with the wireless network, wherein the CCC manages and controls the access points associated with the wireless network. Control frames (MMPDUs, in the case of 802.11 networks) received by the access point can be automatically transferred to the CCC, which thereafter transfers a response back to the access point, thereby granting or denying access to the wireless network to users thereof based on the response transferred from the CCC. The CCC manages radio monitoring to generate a radio mapping of the wireless network and the radio environment thereof based on data received from the access points. A firewall is generally located between the CCC and a visitor gateway. The visitor gateway can communicate with the Internet and restrict access to the wireless network by a visiting user through or from the remote computer network. A plurality of clients can be separated into one or more client groups, with each client group possessing a shared key for accessing networks partitioned from the access point using broadcast frames and encryption. The CCC can arrange the network such that clients ignore broadcast packets for other than its subnetwork.

WO 2003/093951 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/14204

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04L 12/56

US CL : 370/338

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 370/338

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,141,763 A (SMITH ET AL) 31 OCTOBER, 2000, ALL	1-50

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 25 AUGUST 2003	Date of mailing of the international search report 15 SEP 2003
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer KENNETH VANDERPUYE Telephone No. (703) 308-7828

Form PCT/ISA/210 (second sheet) (July 1998)*